REMARKS

Claims 1-6, 10, 14, 16-20 and 22 have hereby been amended to improve form and claims 7 and 23 have been canceled without prejudice or disclaimer. Claims 1-6 and 8-22 are now pending in this application.

Claims 1-23 have been rejected under 35 U.S.C. § 102(b) as being anticipated by Sudia et al. (U.S. Patent No. 5,825,880; hereinafter Sudia). The rejection is respectfully traversed.

Claim 1 recites a method for performing cryptographic-related functions in a network node. Claim 1, as amended, recites executing an application program at the network node, receiving an input requiring cryptographic-related processing, generating a message via the application program based on the input, the message representing one of a predefined set of messages for processing by a cryptographic processing component located within the network node and transmitting the message to the cryptographic processing component. The applicants note that some of these features were previously recited in claim 3.

The Office Action states that Sudia teaches a method for performing cryptographic-related functions that includes receiving an input requiring cryptographic-related processing and generating a message representing one of a predefined set of messages for processing by a cryptographic processing component and points to col. 7, lines 34-52, col. 11, lines 6-15 and col. 9, lines 9-13 for support (Office Action – page 2). The Office Action also states that Sudia discloses transmitting the message to a cryptographic processing component and points to col. 10, lines 5-46 for support (Office Action – page 2).

Sudia is directed to a multi-step signing system that uses multiple signing devices to affix a single signature which can by verified by a public verification key, where each signing device possesses a share of the signature key (Sudia – Abstract). Sudia at col. 7, lines 34-52 discloses that each signing device 39 (Fig. 2) receives requests through a message server 47 that performs routine communication processes, such as stripping off routine privacy envelopes and queuing the inputs. The message server 47 presents messages to the signing device 39, receives the signed result or partially signed result and either returns the partially signed result to the requester or routes the result to the next device in the protocol. This portion of Sudia, however, does not disclose or suggest a method of performing a cryptographic-related processing in a network node that includes the features recited in claim 1.

For example, Sudia discloses that a data center configuration 48 includes a signing device 39 and a separate message server 47. The signing device 39 is located in a physically secure location, such as a vault (Sudia – col. 7, lines 18-24). While data center configuration 48 of Sudia may include signing device 39 and a separate message server 47, Sudia does not disclose that these devices are part of the same network node. In other words, Sudia merely discloses that message server 47 transmits a message to an external signing device 39, which is located at a physically separate location from message server 47. This is not equivalent to generating a message via an application program executed at a network node and transmitting the message to a cryptographic related processing component located within the same network node, as required by amended claim 1.

Sudia at col. 11, lines 6-15 discloses that each signing device generates a private signature key and sends a signature key certification request to administrator 61 (Fig. 4).

The administrator 61 then signs the certification request using the administrator's private signature key. This portion of Sudia also does not disclose or suggest executing an application program at a network node, generating a message via the application program and transmitting the message to a cryptographic processing component located within the same network node, as required by claim 1.

Sudia at col. 9, lines 9-13 refers to Fig. 3 which illustrates a workstation for authorizing agents and an architecture for a trusted device to be used by an authorizing agent. Each workstation 51 includes a smart card reader 53 and each operator has a smart card 55. The smart card 55 includes a crypto unit 46 that is a special purpose arithmetic accelerator unit for performing arithmetic operations for encryption/decryption. This portion of Sudia also does not disclose or suggest executing an application program at a network node, generating a message via the application program and transmitting the message to a cryptographic processing component located within the same network node, as required by claim 1.

Claim 1 also recites performing the cryptographic-related processing by the cryptographic processing component. The Office Action states that Sudia discloses this feature and points to col. 10, lines 5-46 for support (Office Action – page 2).

Sudia at col. 10, lines 5-46 discloses a key distribution procedure in which each signing device receives public encryption and signature verification keys for the other signing devices. This portion of Sudia does not disclose or suggest that the cryptographic signing devices receive a message generated by an application program located within the same network node as the signing device. Therefore, Sudia does not disclose or suggest performing cryptographic-related processing by a cryptographic processing component

that is located within the same network node as the network node executing the application program, as required by claim 1.

For at least the reasons discussed above, Sudia does not disclose or suggest the combination of features of claim 1. Accordingly, withdrawal of the rejection and allowance of claim 1 are respectfully requested.

Claims 2-4 are dependent on claim 1 and are believed to be allowable for at least the reasons claim 1 is allowable. In addition, these claims recite additional features not disclosed or suggested by Sudia.

For example, claim 3, as amended, recites that the generating a message includes generating a function call message via the application program, where the function call message represents a request for performing a predetermined cryptographic-related function. A similar feature was recited in original claim 7. As to the similar feature recited in original claim 7, the Office Action points to col. 7, lines 34-45 of Sudia as allegedly disclosing this feature (Office Action – page 4). The applicants respectfully disagree.

Sudia at col. 7, lines 34-45, as discussed above, discloses that message server 47 presents messages to a signing device 39, receives the signed result and routes the result to the next device. Sending a message to signing device 39 is not equivalent to generating a function call message via an application program. That is, the message server 47 of Sudia merely verifies incoming messages against a list of authorized devices and if the message is verified, presents the message to the signing device 39 (Sudia – col. 8, lines 9-18). Merely passing on a message to a signing device 39 after the message is

verified is not equivalent to generating a function call message via an application program, as required by claim 3.

For at least this additional reason, withdrawal of the rejection and allowance of claim 3 are respectfully requested.

Claim 5, as amended, recites a computer-readable medium that includes instructions that may be invoked by a plurality of predefined message. The instructions cause a processor to perform a method comprising receiving an input representing one of the predefined messages, transmitting, based on the input, a function call representing a request for cryptographic-related processing to a cryptographic processing module executed by the processor and performing the cryptographic-related processing. The applicants note that some of these features were previously recited in claim 7.

Similar to the discussion above with respect to claim 3, Sudia does not disclose transmitting a function call message to a cryptographic processing module, but merely forwards a message received by message server 47 to a signing device 39. Sudia also clearly does not disclose that the same processor that transmits the function call executes the cryptographic processing module, as recited in amended claim 5.

For at least the reasons discussed above, Sudia does not disclose or suggest the combination of features of claim 5. Accordingly, withdrawal of the rejection and allowance of claim 5 are respectfully requested.

Claims 6 and 8 are dependent on claim 1 and are believed to be allowable for at least the reasons claim 5 is allowable. Accordingly, withdrawal of the rejection and allowance of claims 6 and 8 are respectfully requested.

Claim 9 recites a cryptographic module that includes a memory configured to store a plurality of cryptographic processing programs, where each program is invoked via one of a plurality of predefined messages. The cryptographic processing component also includes a processor that is configured to receive an input requiring cryptographic-related processing, generate one of the predefined messages based on the input, transmit the message to a first one of the cryptographic processing programs and perform the cryptographic-related processing.

The Office Action states that Sudia discloses these features and points to col. 9, lines 1-13 and 55-56, col. 11, lines 6-15, col. 8, lines 10-11 and 24-55 and col. 7, lines 34-40 for support (Office Action- pages 4-5). The applicants respectfully disagree.

As discussed above with respect to claim 1, Sudia at col. 7, lines 34-52, col. 11, lines 6-15 and col. 9, lines 9-13, discloses that a separate message server 47 in data center configuration 48 forwards messages to a signing device 39. These portions of Sudia do not disclose or suggest a cryptographic module that includes a memory that stores cryptographic processing programs invoked via one of a plurality of predefined messages and a processor that generates one of the predefined messages based on an input, transmits the message to one of the cryptographic processing programs and performs the cryptographic-related processing, as recited in claim 9.

The additional portions of Sudia referenced above with respect to claim 9 (i.e., col. 9, lines 1-8 and 55-56 and col. 8, lines 10-11 and 24-55) also do not disclose or suggest these features.

For example, Sudia at col. 9, lines 1-8 discloses that memory 52 on a smart card 55 includes areas for storing system firmware 43, device keys, 45, user keys 47,

application firmware 49 and a work area 54. Sudia at col. 9, lines 55-56 discloses that signing devices encrypt communications using public/private cryptographic schemes. These portions of Sudia do not disclose or suggest a cryptographic module that includes a memory that stores a plurality of cryptographic processing programs invoked via one of a plurality of predefined messages. These portions of Sudia also do not disclose or suggest a processor that receives an input, generates one of the predefined messages, transmits the message to a first cryptographic processing program and performs the cryptographic-related processing, as required by claim 9.

Sudia at col. 8, lines 10-11 discloses that message server 47 verifies all messages against a list of authorized devices including signing devices and authorizing agents. Sudia at col. 8, lines 24-55 discloses that workstations include a smart card reader 53 and operators each have secure smart cards 55. Each smart card 55 contains a private decryption key and a private signature key that are unique to that smart card 55. These portions of Sudia do not disclose or suggest a cryptographic module that includes a memory that stores a plurality of cryptographic processing programs invoked via one of a plurality of predefined messages. These portions of Sudia also do not disclose or suggest a processor that receives an input, generates one of the predefined messages, transmits the message to a first cryptographic processing program and performs the cryptographic-related processing, as required by claim 9.

For at least the reasons discussed above, Sudia does not disclose or suggest the combination of features of claim 9. Accordingly, withdrawal of the rejection and allowance of claim 9 are respectfully requested.

Claims 10-12 are dependent on claim 9 and are believed to be allowable for at least the reasons claim 9 is allowable. In addition, these claims recite additional features not disclosed or suggested by Sudia.

For example, claim 11 recites features similar to claim 3. For reasons similar to those discussed above with respect to claim 3, Sudia does not disclose or suggest the features of claim 11.

For at least this additional reason, withdrawal of the rejection and allowance of claim 11 are respectfully requested.

Claim 13 recites features similar to claim 9 in means plus function form. For reasons similar to those discussed above with respect to claim 9, withdrawal of the rejection and allowance of claim 13 are respectfully requested.

Claim 14 recites features similar to claim 1. For reasons similar to those discussed above with respect to claim 1, withdrawal of the rejection and allowance of claim 14 are respectfully requested.

Claims 15-21 are dependent on claim 14 and are believed to be allowable for at least the reasons claim 14 is allowable. Accordingly, withdrawal of the rejection and allowance of claims 15-21 are respectfully requested.

Claim 22 recites a computer-readable medium that stores instructions executable by at least one processor to perform a method for providing cryptographic-related functions. The method includes receiving a first function call from a predefined list of function calls, the predefined list of function calls representing available cryptographic-related functions executable by the at least one processor, generating a request message based on the first function call, the request message representing a request for processing

by a cryptographic processing module executed by the at least one processor, transmitting the request message to the cryptographic processing module and performing the cryptographic-related function.

The Office Action states that Sudia discloses these features and points to col. 8, lines 10-11, col. 11, lines 6-15 and col. 9, lines 9-13 and 55-56 for support (Office Action – page 7). The applicants respectfully disagree.

The above-cited portions of Sudia merely disclose that a message server 47 may verify incoming messages against a list of authorized devices before forwarding the messages to a signing device 39 (col. 8, lines 10-11), signing devices generate a private signature key for transmission to administrator 61, that signs each request using a private key (col. 11, lines 6-15) and smart card 55 includes areas for storing keys, firmware 49 and a crypto-unit 46 (col. 9, lines 9-13 and 55-56). None of these portions of Sudia, or any other portions, discloses or suggest a computer-readable medium that causes a processor to perform a method that includes receiving a first function call from a predefined list of function calls, where the predefined list of function calls represents available cryptographic-related functions executable by the at least one processor, as recited in claim 22. In contrast, Sudia merely discloses receiving conventional request messages and passing on the request messages to a signing device.

None of the above-cited portions of Sudia further disclose or suggest generating a request message based on the first function call, the request message representing a request for processing by a cryptographic processing module executed by the at least one processor, as recited in amended claim 22. In addition, none of these portions of Sudia

disclose or suggest transmitting the request message to the cryptographic processing module and performing the cryptographic-related function, as recited in claim 22.

For at least the reasons discussed above, Sudia does not disclose or suggest the combination of features of claim 22. Accordingly, withdrawal of the rejection and allowance of claim 22 are respectfully requested.

CONCLUSION

In view of the foregoing amendments and remarks, the applicants respectfully request withdrawal of the outstanding rejections and the timely allowance of this application.

To the extent necessary, a petition for an extension of time under 37 C.F.R. § 1.136 is hereby made. Please charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, to Deposit Account 07-2347 and please credit any excess fees to such deposit account.

Respectfully submitted,

By: _____
Joel Wall
Reg. No. 25,648

Date: June 29, 2004
Verizon Corporate Services Group Inc.
600 Hidden Ridge Drive
Mail Code HQE03H14
Irving, Texas 75038
(972) 718-4800
CUSTOMER NO. 32127